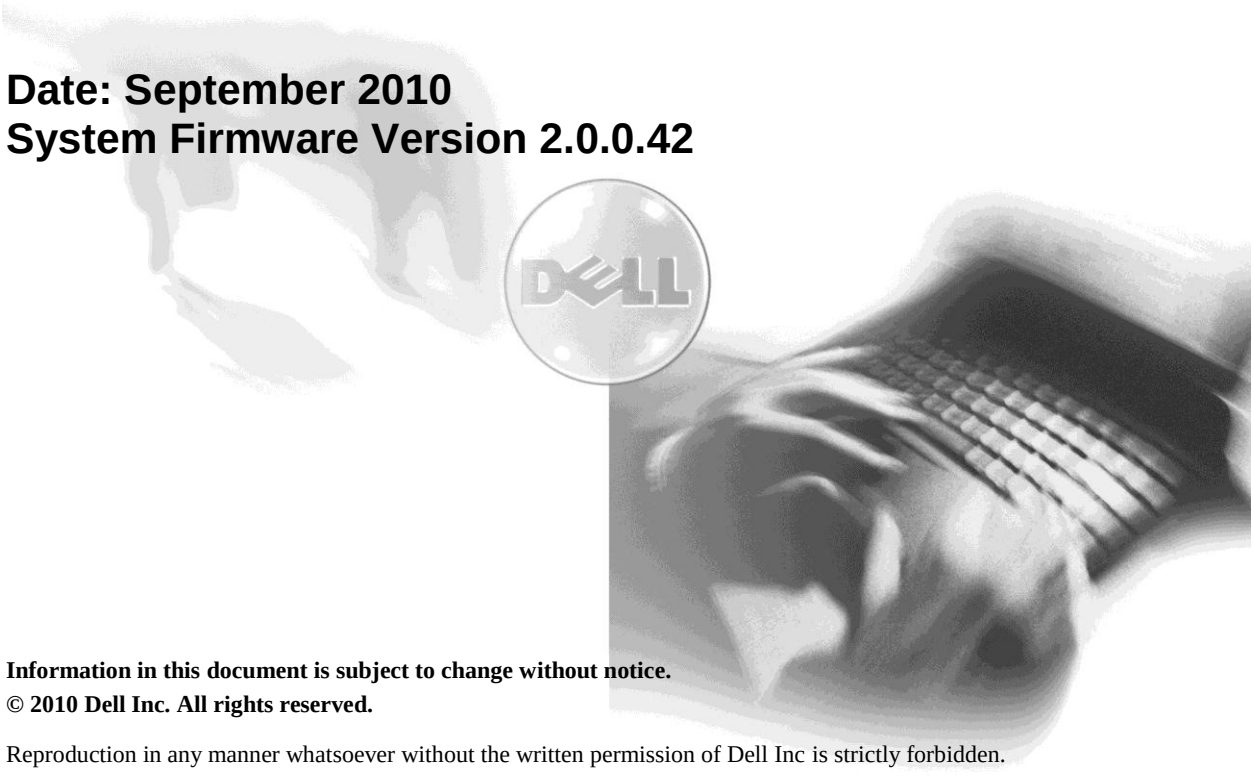
Dell™ PowerConnect™ 3524/3548/3524P/3548P

PowerConnect 3524/3548/3524P/3548P Release Notes

Date: September 2010
System Firmware Version 2.0.0.42



Information in this document is subject to change without notice.
© 2010 Dell Inc. All rights reserved.

Reproduction in any manner whatsoever without the written permission of Dell Inc is strictly forbidden.

Trademarks used in this text: Dell, the DELL logo and PowerConnect are trademarks of Dell Computer Corporation; Microsoft and Windows are registered trademarks of Microsoft Corporation.

Other trademarks and trade names may be used in this document to refer to either the entity claiming the marks and names or their products. Dell Computer Corporation disclaims any proprietary interest in trademarks and trade names other than its own. All rights reserved. This document may not, in whole or in part, be copied, photocopied, reproduced, translated, or reduced to any electronic medium or machine readable form without the prior written consent of Dell. Dell reserves the right to make changes without further notices to any products or specifications referred to herein to improve reliability, functionality or design. Reproduction, adaptation or translation without prior written permission is prohibited, except as allowed under the copyright laws.

Table of Contents

Introduction 1

GLOBAL SUPPORT 1

Firmware Specifications 1

Added functionality in this release 1

Issues resolved 2

Known Restrictions and Limitations 4

auto-negotiation on Port Channel/s with fiber port/s....4

Voice VLAN Will not activate automatically on port which is in up state....4

MSTP doesn't treat invalid Version number....4

Duplex LED....4

SFP Ports....4

System Usage Notes 4

Non-Present Ports....4

Ports are not removed automatically from an IGMP group by removing them from the VLAN....4

Only management stations with super community access can set rndAlarmEnabling....4

Broadcast Storm Control Ranges....4

Queue Settings on Cascaded/Stacked Ports....5

SNTP Interface Polling....5

mac address will be learned even if mac-acl denies the address / traffic....5

jabbers are counted as frames of 1632 bytes instead of oversize packets....5

Oversize packets are counted according to MAX packet size 1632 octets, no matter what is the real packet size....5

rmon statistics: frames of xx bytes will be counted as transmitted from port and received to port....5

PVE Limitations: FE port can not be an UpLink....5

Device does not learns maximum MAC entries....5

Login Banner....5

Telnet....6

Bind MAC to VLAN....6

End of Release Notes 6

PowerConnect 3524/3548 Release Notes

Introduction

This document provides specific information for the Dell PowerConnect 3524/3548/3524P/3548P Switch system, firmware version 2.0.0.42.

It is recommended that this release note be thoroughly reviewed prior to installing or upgrading of this product.

GLOBAL SUPPORT

By Web: http://support.dell.com/

For information regarding the latest available firmware, recent release notes revisions, or additional assistance, please visit the http://www.dell.com Support Web Site.

Firmware Specifications

Firmware Version Details

Boot PROM Name	Version No.	Release Date
powerconnect_35xx_boot-20000.rfb	2.0.0.0	September, 2008

Firmware Image Name	Version No.	Release Date
powerconnect_35xx-20042.ros	2.0.0.42	Sept, 2010

The firmware image version should be 2.0.0.42 on the PowerConnect 3524/3548/3524P/3548P. The boot prom image should be 2.0.0.0 Refer to the PowerConnect 35XX Systems User's Guide for instructions on loading the boot PROM software and updating the firmware image.

Version Numbering Convention					
Version number					**Description**
3524/3548/ 3524p/3548P	2	0	0	42	Four part version number
				↑	Denotes the build number.
			↑		Denotes an ad hoc release of the product software.
		↑			Denotes a scheduled maintenance release of the product software.
	↑				Denotes a major version number.

Supported Firmware Functionality

For more details regarding the functionalities listed, please refer to the PowerConnect 35XX Systems User's Guide.

Added functionality in this release

The following new feature was added to the 2.0.0.42 version release of the PowerConnect 35XX:

SSL Default Supported Version – By default the device supports only versions starting with SSLv3. By using a CLI command the user can enable SSLv2 such that both SSLv2 & SSLv3 are supported.

In order to enable/disable the support of SSLv2 the user should use the CLI command '**ssl version [v2&v3 / v3]**'

In order to show the current SSL versions which are supported the user can use the CLI command **'show ssl version'**

Issues resolved

The following is a list of issues resolved between 2.0.0.40 and 2.0.0.42

Description	User Impact	Resolution
In the case of Concurrent telnet connections, part of the switch configuration might not be displayed in one or more of the telnet connections.	If more than 1 user is connected via telnet and using show commands - user may need to repeat the show commands in order to display all relevant information.	Fixed
When using the show running and show startup commands the device Console does not display information on the version number and service tag	Version number and service tag are missing from CLI show running command	Fixed
When using the show running and show startup commands the device Console does not display information on the version number and service tag	Version number and service tag are missing from CLI show running command	Fixed
In a network with a few switches with equal STP Bridge Priority values – in some cases a switch with the higher MAC address will be elected as the STP root bridge	A switch which should not have been elected Root Switch will become root switch, affecting network STP topology	Fixed – If STP Bridge Priority is equal, the switch with the lower MAC address will be elected as STP Root Bridge for all MAC address range Note: to assure proper STP operation in the network – all devices in network should be upgraded to the new version.
Device ID information which is received through LLDP protocol is displayed as "Garbage" characters in the Web GUI	In order to show the device ID received by the LLDP protocol the user need to use show command in the Command Line Interface	Fixed – the same device ID is displayed in the CLI and the Web GUI

The following is a list of issues resolved between 2.0.0.29 and 2.0.0.40 firmware release.

Description	User Impact	Resolution
When device is in stack configuration (2 units or more), Serial Console freezes if more than 2 copper SFPs are inserted to SFP slots.	Console will freeze after CLI commands entered , and user will not have access to CLI until Copper SFPs are removed Note: occurs only if there is no “link up” on copper SFP interface	Fixed
When traffic shaping is enabled on a port, the port will sometimes stop forwarding traffic	Devices and users connected to these ports loose connectivity with network. Device needs to be rebooted to renew connectivity.	Fixed.
LLDP malfunctions when there are more than 30 LLDP-MED endpoints	If more than 30 LLDP-MED endpoints (such as VoIP phones) are connected to switch they will randomly loose LLDP-MED configuration, causing disruption in functionality.	Fixed.

'Show IPv6 tunnel'	The 'show ipv6 tunnel' CLI command does not include all info; such as enable/disable status	Command output was extended to include: tunnel Status, Tunnel Protocol, Tunnel Local Address Type and Tunnel Local IPv4 Address Type
After more than 100 TFTP downloads, The tftp copy fails	After many tftp downloads (around 100) - tftp copy fails with message "%TFTP-C-OPEN: No free UDP port"	Fixed.
SFP ports don't work in SA mode	SFP links do not function when device is operating in standalone mode	Fixed.
Device reboots after long period of time	The device reboots with the message: "FATAL ERROR: SW2M: ABORT DATA exception"	Fixed.
Fiber ports at reboot	Stack is stuck with 100% CPU utilization when rebooting connected to another Ryan stack using fiber ports	Fixed
Counters support	Missing support for MIB counters ifOutErrors on FE ports	support for MIB counters ifOutErrors was added
Banner configuration – error messages	Need to change format of Banner error message when user enters more than 80 characters in a single line so it will be clearer	Format of Banner message was changed to "This line is longer than 80 characters and therefore will be displayed in multiple lines."; error message will be displayed immediately following line input
Banner configuration – error messages	Need to add error message to all banner commands if single line input exceeds 511 characters	The following error message was added: "This line is longer than 511 characters and therefore it is not accepted and will not be displayed." The error message will be displayed immediately following line input Note: the whole line is not accepted and needs to be re-entered.
CLI command support	SNMP host command does not allow user to configure zone ID for IPv6 SNMP servers	Fixed; SNMP (and other) host command allows user to configure zone ID for IPv6 SNMP servers; "RADIUS" was replaced in relevant CLI Help lines.
Home Page	When fiber are configured as stacking ports - home page showed both fiber and copper ports as g3 and g4	Fixed

Known Restrictions and Limitations

Title	Description
auto-negotiation on Port Channel/s with fiber port/s	Port Channel/s with fiber port/s can not be configured with “auto-negotiation” mode. Work Around: Port Channel/s with fiber port/s should be configured by user to “no auto-negotiation”.
Voice VLAN Will not activate automatically on port which is in up state	Voice VLAN is based on the FDB MAC table learning mechanism. To allow correct operation please first configure the feature and only then connect the VoIP equipment. Work Around: To clean FDB table and cause the device to relearn MAC addresses.
MSTP doesn’t treat invalid Version number	MSTP BPDUs with version number 1 are processed by device when in MSTP mode, which is incorrect. The correct behavior is not to not use the information for path calculation. This is a minor, test scenario issue, which was not reported from the field. Work Around: None.
Duplex LED	Duplex LED remains lit if port duplex mode is set to full and port settings are changed. This is true even after link is disconnected. Work Around: None
SFP Ports	SFP ports cannot be activated when in standalone mode. Work Around: Set unit to work in stacking mode (single unit with unit ID #1 or #2)

System Usage Notes

Title	Description
Non-Present Ports.	Certain ports in the device may have a status of "non-present ports" in CLI show commands. These include: - The stacking ports can be presented as user ports, in the event that the device is a standalone (and not a stack unit). Therefore, these ports are treated as "non-present" when in stacking mode. - 100Mb ports 25-48 of a 24-port device are considered "non-present" ports, so that in the event of hot insertion of a 48-port device in place of the 24-port device, the ifindexes of the GE ports remain consistent.
Ports are not removed automatically from an IGMP group by removing them from the VLAN.	Ports are not removed from MAC Multicast Address table, when they are removed from the VLAN. Ports are added to the MAC Multicast Address Table by using the command **bridge multicast address** *ip-address* **add** *interface*. Ports must be proactively removed from the MAC Multicast Address Table by using the command **bridge multicast address** *ip-address* **remove** *interface*.
Only management stations with super community access can set rndAlarmEnabling.	Only management stations with super community access can set rndAlarmEnabling.It is not possible to set rndAlarmEnabling when rw community is defined for the Default View.
Broadcast Storm Control Ranges	Storm control rates refer to the average number of bytes over a period of time. This period of time decreases as the configured rate increases. For example, configuring a rate of 70 kbps results in a rate of 70 kbps over an average of 1 minute. From rate of 100kbps it becomes steady.

Queue Settings on Cascaded/Stacked Ports	The system can be set to work in either Strict Priority or WRR. This applies to cascading and stacking ports as well. In order to be able to handle high priority traffic across the cascaded links. From an implementation perspective cascaded ports are set to SP. Unicast traffic was assigned to the high priority queue. Therefore, if Unicast traffic is sent at wire-speed, it is prioritized over broadcast traffic to the CPU. This is not a real-life scenario.
SNTP Interface Polling	If the IP interface is configured on a physical interface (port, LAG), which goes to down, the device continues to poll until the timer expires. If the physical interface goes up again, the unit will not continue to poll. Consider, for example, a case of a stack in which an IP interface is configured on a physical interface of the backup unit (or any other unit). If that unit is severed from the stack, the master unit continues to poll until the timer expires. After that, it ceases polling, even if the backup unit is reconnected to the stack. Work Around: It is recommended to configure SNTP servers on the default VLAN. If you have not configured SNTP servers as recommended, use the Global Configuration command ***clock source sntp*** to re-activate the server.
mac address will be learned even if mac-acl denies the address / traffic	On 100Mb ports MAC address learning will occur even with rule "deny any any" (but traffic will not be forwarded) Work Around: None.
jabbers are counted as frames of 1632 bytes instead of oversize packets	Jabbers are counted as frames of 1632 bytes instead of oversize packets. It is only a counter issue. Work Around: None.
Oversize packets are counted according to MAX packet size 1632 octets, no matter what is the real packet size.	The MAX packet size is 1632. Counting of oversized packets is done according to this value multiplied by the number of wrong packets. Work Around: None.
rmon statistics: frames of xx bytes will be counted as transmitted from port and received to port	rmon statistics: transmitted packets are counted as well as received packets. Work Around: None.
PVE Limitations: FE port can not be an UpLink	Device gives error message when trying to configure the 100MB port as Uplink Port. The PVE Uplink_Port Must have higher throughput than PVE protected ports. Work Around: None
Device does not learns maximum MAC entries	The System does not learn the maximum entries of 8K in MAC address table, but only 7936. When several different MAC addresses generate an identical Hash result, a hash-collision resolution operation is carried out. However, this mechanism has finite capacity; under rare situations, the system will not be able to resolve hash-collisions, and so will be unable to store the new address in the hardware table, and it will not be learned. Under these conditions, it may appear to the user that fewer addresses may be accommodated Work Around: None
Login Banner	Configuration of the Login Banner is not supported via cut & paste operation and requires use of designated CLI commands.

Telnet	IE7.0 does not support the telnet API
Bind MAC to VLAN	This feature was deprecated in this release and replaced by Dynamic VLAN Assignment (DVA)

End of Release Notes